REMARKS

The Examiner is thanked for the performance of a thorough search.

Claims 1, 8, 12, 18, 20-21, 24-25, 28-29, and 32 have been amended. No claims have been canceled or added. Hence, Claims 1, 4-21, 23-25, 27-29, 31-32, 34-37, 39-42, and 44-47 are pending in the present application.

Each issue raised in the final Office Action mailed March 18, 2009 is addressed hereinafter.

I. ISSUES NOT RELATING TO PRIOR ART

A. AMENDMENTS TO THE SPECIFICATION

The Specification has been amended herein to include the language of Claims 1, 2, 3, 4, and 20 as originally filed. Thus, it is respectfully submitted that the present amendment to the Specification does not introduce new matter, but merely incorporates into the specification the language of several originally filed claims. For this reason, entry of the present amendment to the Specification is respectfully requested.

B. REJECTIONS UNDER 35 U.S.C. § 112, FIRST PARAGRAPH

Claims 1, 21, 25, and 29 were rejected under 35 U.S.C. § 112, first paragraph as allegedly failing to comply with the written description requirement. This rejection is respectfully traversed.

The Office Action asserts that the Specification as originally filed and the original claims did not describe "defining a number of required signatures and required principals." This assertion is incorrect because this feature is expressly recited in each of the original Claims 3-4 and 13-14. Further, the original Claims 3-4 and 13-14 further include a feature that specifies a particular functionality that is performed based on the defined number of required signatures and required principals, namely "applying the particular configuration directive only when the

configuration information has the number of required signatures by the required principals". Thus, it is respectfully submitted that the Specification and the claims as originally filed described the feature of "security information defining a number of required signatures and required principals" in a way that clearly and more than reasonably conveys to one skilled in the art that the Applicant had possession of this feature at the time the present application was filed.

Nevertheless, in order to further the prosecution of the present application, the language of the original Claims 3 and 4 has been incorporated in the Specification through the specification amendment provided concurrently herewith. Thus, it is respectfully submitted that as amended the Specification has full and literal support for the above-referenced feature.

For the foregoing reasons, reconsideration and withdrawal of the rejections of Claims 1, 21, 25, and 29 under 35 U.S.C. § 112, first paragraph is respectfully requested.

II. ISSUES RELATING TO THE CITED ART

A. INDEPENDENT CLAIM 1

Claim 1 was rejected as allegedly unpatentable under 35 U.S.C. § 103(a) over Bosler, U.S. Patent Application Publication No. US 2005/0010757 ("BOSLER") in view of Kinnis et al., U.S. Patent No. 6,959,382 ("KINNIS"). The rejection is respectfully traversed.

Among other features, Claim 1 comprises the features of:

> **receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals;**
> **receiving configuration information comprising** a hostname, **one or more configuration directives** for a host network element associated with the hostname, and **two or more digital signatures** of the hostname and configuration directives;
> ... ;
> wherein the two or more digital signatures comprise **a first digital signature** of **a first portion** of the **one or more configuration directives** by a **first user**, and a **second digital signature** of a **second portion** of the **one or more configuration directives** by a **second user**;
> **verifying** that the two or more digital signatures are valid and **that two or more principals respectively associated with the two or more digital signatures**

have collective authority to perform the configuration directives on the host network element;

applying the configuration directives to the host network element only when the two or more digital signatures are verified successfully;

wherein applying the configuration directives comprises **applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals**.

It is respectfully submitted that BOSLER and KINNIS do not describe or suggest the features of Claim 1 that are highlighted above.

Claim 1 includes the feature of receiving configuration information that comprises (among other things) one or more configuration directives for a host network element and two or more digital signatures, where the two or more digital signatures comprise a first digital signature of **a first portion** of the one or more configuration directives by a first user, and a second digital signature of a **second portion** of the one or more configuration directives by a second user. Thus, this feature of Claim 1 indicates that, within the same configuration information, a first portion of the configuration directives is signed with a first digital signature by a first user and a second portion of the configuration directives is signed with a second digital signature by a second user. In the rejection of Claim 20, the final Office Action asserts that KINNIS describes this feature of Claim 1. This assertion is incorrect.

In col. 3, lines 3-30, KINNIS expressly describes that a digital service provides for multiple signatories related to a single document. Significantly, after a first user generates a first signature file that includes the signature, the document, and the certificate of the first user, a second user can generate a second signature file that encapsulates the first signature file and contains the digital signature of the second user. In other words, both the first signature of the first user and the second signature of the second user are applied to the entire document. Further, it is respectfully submitted that KINNIS does not describe or suggest that its digital service can sign different portions of the same thing (such as a document) with the digital signatures of

different users. On the contrary, numerous passages of KINNIS expressly describe that any digital signature is applied to and authenticates the entire document being signed, including digital signatures that are applied to files that may include the document along with other users' signatures. For example, with respect to its Fig. 9, in col. 10, lines 48-50 and 64-66 KINNIS expressly describes that any subsequent signatures are applied to and encapsulate the entire signature file that includes a previously signed document.

In contrast, the above features of Claim 1 indicate that, within the same configuration information, two or more digital signatures comprise a first digital signature of **a first portion** of the configuration directives by a first user, and a second digital signature of a **second portion** of the **same** configuration directives by a second user. Since KINNIS does not describe that its digital service can sign different portions of the same document with the digital signatures of different users, KINNIS does not describe these features of Claim 1. Further, it is noted that BOSLER does not cure this deficiency of KINNIS because BOSLER does not describe or even suggest that multiple signatures are used to sign any management message in BOSLER's network management system.

In addition, Claim 1 comprises the features of: receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals; and applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals. The final Office Action asserts that BOSLER describes these features of Claim 1 in paragraphs [0058] and [0069]. This assertion is incorrect.

Neither paragraphs [0058] and [0069] nor any other paragraph of BOSLER describes or suggests that a management message includes a number of required signatures and required principals, where the number may be used in determining whether to apply a configuration

command. Moreover, while in paragraph [0069] BOSLER may be describing that a management server may be capable of sending management requests to the nodes being managed, BOSLER does not describe that the management server checks or otherwise determines anything about a number of required signatures and required principals that are associated with a management request. In fact, it appears that paragraphs [0058] and [0069] of BOSLER refer to two completely different and separate embodiments – the embodiment in paragraph [0058] refers to establishing secure sessions between nodes by exchanging a management message, while the embodiment in paragraph [0069] refers to a management server that sends management requests to nodes that are being managed.

In contrast, Claim 1 comprises the features of receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals; and applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals. According to these features of Claim 1, a particular configuration directive is applied only when the configuration information (which includes the particular configuration directive) has the number of required signatures and principals, which number is specified in previously received security information.

The final Office Action also asserts that KINNIS describes the feature of Claim 1 of verifying that the two or more digital signatures are valid and that two or more principals respectively associated with the two or more digital signatures have collective authority to perform the configuration directives on the host network element. Specifically, on page 3 the final Office Action asserts that the collective authority to perform the configuration directives of Claim 1 is equivalent to the verification of each digital signature in KINNIS because the

verification of each digital signature is required in order to authenticate the original document. These assertions are incorrect.

In col. 3, lines 3-24, KINNIS describes a digital signature service that can be used by multiple users to sign a single document. A first user invokes the digital signature service to generate a first signature file corresponding to the document. After receiving the first signature file, a second user (e.g., a party to a contract with the first user) verifies through the digital signature service that the content of document is not altered and authenticates the first user as the user who digitally signed the document. Then, if the second user wishes to digitally sign the document, the second user may invoke the digital signature service to generate a second signature file for the document. In col. 10, lines 38-67, KINNIS further describes that a third user may also wish to become signatory to the document. The third user invokes the digital signature service to verify the contents of the document and to verify the authenticity of the second user and of the first user. If the third user then wishes to become a signatory to the document, the third user invokes the digital signature service to sign the document that was signed by the second user.

Significantly, however, KINNIS does not describe or suggest anything about verifying whether the two or three users have **collective authority** to perform any configuration directives on a network element, as featured in Claim 1. It is noted that verifying multiple signatures to authenticate a document is irrelevant to this feature of Claim 1 because authenticating a document (as described in KINNIS) is quite different from verifying whether two or more users have collective authority to perform certain operations on a network element (as featured in Claim 1). For example, a message with configuration directives may be determined as being authentic (e.g., as being sent from a valid administrator account), yet the configuration directives therein may come from users (e.g., lower-level administrators) that are not authorized to perform

the directives on a particular network element (e.g., a core router).

While KINNIS may be describing that two or three users may digitally sign the same document separately from each other, KINNIS does not describe or suggest that the two or three users have any collective authority that they can convey by singing the same document. Rather, KINNIS describes that any user who wishes to digitally sign the document may do so by using the digital signature service. (See, for example, KINNIS col. 10, lines 27-29, 41-45, 53-54, and 60-64.) In other words, KINNIS describes that each user may have authority to sign a document separately and independently from any other user. Further, while the users in KINNIS may digitally sign a document with digital signatures, KINNIS does not describe that these digital signatures are used in any way to determine whether the users have some authority to perform any action, such as applying configuration directives as featured in Claim 1. Rather, the users in KINNIs digitally sign the document in order to verify the integrity of the document and the authenticity of the user signing the document. (See, for example, KINNIS, col. 2, lines 32-36.)

In contrast, Claim 1 comprises the feature of verifying that the two or more digital signatures are valid and that two or more principals respectively associated with the two or more digital signatures have collective authority to perform the configuration directives on the network element. It is respectfully submitted that verifying the integrity of a document and authenticating the users that digitally signed the document (as described in KINNIS) is not equivalent to verifying that two or more principals have collective authority to perform configuration directives on a network element (as featured in Claim 1).

Finally, the Applicant previously argued that there is no rational reason or other evidentiary underpinning for modifying the BOSLER system to use multiple digital signatures as described in KINNIS, as is required to sustain an obviousness rejection under 35 U.S.C § 103(a). Specifically, the Applicants argued that since BOSLER describes using a digital signature for the

purpose of authenticating a sender node, the sender node does not need to send more than one signature in order to authenticate itself with the receiving node. In fact, BOSLER does not describe or suggest that a node may be assigned more than one private key, which means that in BOSLER a node cannot sign a management message with more than one digital signature. Thus, one of ordinary skill in the art would have absolutely no reason, need, or rationale whatsoever for modifying the BOSLER system to use multiple digital signatures as described in KINNIS.

The present Office Action, however, does not address this argument of the Applicant and does not provide a rational reason or other evidentiary underpinning about why one of skill in the art would decide to modify the BOSLER system to use multiple digital signatures as described in KINNIS, given the fact that the BOSLER system uses a digital signature for the sole purpose of authenticating a sender node. Instead, in pp. 4-5, numbered paragraph 3.6, the final Office Action asserts that there is no disclosure in KINNIS that discredits or discourages the usage of any type of combined authority and KINNIS does not teach away from usage of multiple signatures. Even if these assertions in the final Office Action were true, the final Office Action still does not indicate why one of ordinary skill in the art would go to the trouble of overcoming the numerous technical challenges and difficulties that are involved in modifying the BOSLER system to use multiple digital signatures as described in KINNIS, when the use of a single digital signature to authenticate a sender node is completely sufficient in the BOSLER system.

For the above reasons, BOSLER and KINNIS do not describe or suggest all features of Claim 1. Thus, Claim 1 is patentable under 35 U.S.C. § 103(a) over BOSLER in view of KINNIS. Reconsideration and withdrawal of the rejection of Claim 1 is respectfully requested.

B. INDEPENDENT CLAIM 8

Claim 8 was rejected as allegedly unpatentable under 35 U.S.C. § 103(a) over BOSLER in view of KINNIS, and further in view of Sudia et al., U.S. Patent Application Publication No.

US 2002/0013898 ("SUDIA"). The rejection is respectfully traversed.

Among other features, Claim 8 comprises the features of:

> receiving **configuration control information** that **includes a time period during which a valid digital signature is required for applying one or more particular configuration directives**;
> …;
> **only when the date-time value is within the time period and the one or more configuration directives have not been previously received during the time period, attempting to verify the one or more digital signatures** based on the trust information, **and applying the configuration directives** to a network element only when the one or more digital signatures are verified successfully.

The final Office Action asserts that the above features of Claim 8 are described in paragraphs [0071] and [0073] of BOSLER and in paragraph [0249] of SUDIA. Specifically, in p. 4, numbered paragraph 3.4, the final Office Action asserts that the time limit for a certificate as described in paragraph [0249] of SUDIA corresponds to the time period featured in Claim 8. These assertions are incorrect.

It is respectfully submitted that the time limit for a certificate (as described in paragraph [0249] of SUDIA) does not correspond to the time period featured in Claim 8. In SUDIA, the time limit is tied to a particular certificate and is used to determine whether that particular certificate is valid. If the particular certificate is valid, then a delegate user can use a card that stores that particular certificate. (See SUDIA, paragraph [0250].) In contrast, Claim 8 features a time period during which a check must be made to determine whether the same configuration directives have already been received. In other words, the time period featured in Claim 8 prevents the applying of the same configuration directives multiple times within the specified time period. Thus, the differences between the functionality of the time limit for the certificate of SUDIA and the functionality of the time period of Claim 8 are significant. For example, in SUDIA as long as the time limit of a particular certificate has not expired, a delegate user can use a card with that particular certificate to sign any number of document as many times as

necessary. (See, for example, SUDIA, paragraphs [0248] and [0250].) In contrast, the above features of Claim 8 indicate that the same configuration directives will be applied only once during the time period specified in a configuration control information that is received at a host network element.

Further, in response to the previous Office Action, the Applicant argued that BOSLER does not describe the above features of Claim 8 at least because the time period during which a valid signature is required for applying a configuration directive on a network element (as featured in Claim 8) is completely different from a time interval used to determine whether or not a node would be granted a public key certificate (as featured in BOSLER). However, the present final Office Action maintains the same rejection, but does not respond to the Applicant's arguments.

Specifically, in response to the previous Office Action, the Applicant argued that the time interval described in paragraph [0071] of BOSLER is an interval within which a node must request a public key certificate. Significantly, a certificate server would grant a public key certificate to a node only if the node requests the certificate within a particular time interval after a management agent is initialized/installed on the node. (See also at least BOSLER, paragraph [0010]; paragraph [0073], lines 17-22.) Thus, the time interval described by BOSLER is used to determine whether or not a node would be granted a public key certificate, which is very different from a time period for applying configuration directives on a host network element as featured in Claim 8. Further, in paragraph [0058] BOSLER describes that a first node and a second node may establish a secure session by exchanging a management message that may be authenticated by a digital signature. However, BOSLER does not describe or suggest that a management message sent by the first node includes any time interval. In fact, there is absolutely nothing in BOSLER that describes or suggests that management messages exchanged

between nodes may include any time intervals indicating that configuration operations specified in the messages can be applied on nodes only during these time intervals. In contrast, the time period featured in Claim 8 is used to determine whether verification of one or more digital signatures would be attempted and whether one or more configuration directives would be applied to a network element.

Further, as discussed above, SUDIA fails to cure the deficiencies of BOSLER with respect to the above features of Claim 8 because the time limit for a certificate (as described in SUDIA) does not correspond to the time period featured in Claim 8. Specifically, it is noted again that the features of Claim 8 indicate that the time period received in the configuration control information is used to prevent the application of the same one or more configuration directives more than once during that time period. In contrast, the time limit described in SUDIA is used to perform a completely different functionality, namely to limit the period of time during which a delegate user can use a substitution certificate to sign documents on behalf of the primary user.

For the above reasons, BOSLER, KINNIS, and SUDIA do not describe or suggest all features of Claim 8. Thus, Claim 8 is patentable under 35 U.S.C. § 103(a) over BOSLER in view of SUDIA. Reconsideration and withdrawal of the rejection of Claim 8 is respectfully requested.

C. INDEPENDENT CLAIM 18

Claim 18 was rejected as allegedly unpatentable under 35 U.S.C. § 103(a) over BOSLER in view of KINNIS and further in view of SUDIA.

Claim 18 includes features similar to the features of Claim 8 discussed above. Thus, Claim 18 is patentable under 35 U.S.C. § 103(a) over BOSLER in view of KINNIS and further

in view of SUDIA for at least the reasons given above with respect to Claim 8. Reconsideration and withdrawal of the rejection of Claim 18 is respectfully requested.

D. INDEPENDENT CLAIMS 21, 25, AND 29

Claims 21, 25, and 29 were rejected as allegedly unpatentable under 35 U.S.C. § 103(a) over BOSLER in view of KINNIS.

Claims 21, 25, and 29 include features similar to the features of Claim 1 discussed above, except in the context of an apparatus and a computer-readable medium. Thus, Claims 21, 25, and 29 are patentable under 35 U.S.C. § 103(a) over BOSLER in view of KINNIS for at least the reasons given above with respect to Claim 1. Reconsideration and withdrawal of the rejection of Claims 21, 25, and 29 is respectfully requested.

E. DEPENDENT CLAIMS 4-7, 9-17, 19-20, 23-24, 27-28, 31-32, 34-37, 39-42, AND 44-47

Claims 4-7, 23-24, 27-28, 31-32, 34-37, 39-42, and 44-47 were rejected as allegedly unpatentable under 35 U.S.C. § 103(a) over BOSLER in view of KINNIS. Claims 9-17 and 19-20 were rejected as allegedly unpatentable under 35 U.S.C. § 103(a) over BOSLER in view of KINNIS and further in view of SUDIA.

Each of Claims 4-7, 9-17, 19-20, 23-24, 27-28, 31-32, 34-37, 39-42, and 44-47 depends from one of independent Claims 1, 8, 18, 21, 25, and 29, and thus includes each and every feature of the independent base claim. Thus, each of Claims 4-7, 9-17, 19-20, 23-24, 27-28, 31-32, 34-37, 39-42, and 44-47 is allowable for at least the reasons given above for Claims 1, 8, 18, 21, 25, and 29. In addition, each of Claims 4-7, 9-17, 19-20, 23-24, 27-28, 31-32, 34-37, 39-42, and 44-47 introduces one or more additional features that independently render it patentable. However, due to the fundamental differences already identified, to expedite the positive resolution of this case a separate discussion of those features is not included at this time.

Therefore, it is respectfully submitted that Claims 4-7, 9-17, 19-20, 23-24, 27-28, 31-32, 34-37, 39-42, and 44-47 are allowable for the reasons given above with respect to Claims 1, 8, 18, 21, 25, and 29. Reconsideration and withdrawal of the rejections of Claims 4-7, 9-17, 19-20, 23-24, 27-28, 31-32, 34-37, 39-42, and 44-47 is respectfully requested.

III. CONCLUSION

The Applicant believes that all issues raised in the final Office Action have been addressed. Further, for the reasons set forth above, the Applicant respectfully submits that allowance of the pending claims is appropriate. Entry of the RCE filed concurrently herewith and reconsideration of the present application are respectfully requested in light of the amendments and remarks herein.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

A petition for extension of time, to the extent necessary to make this reply timely filed, is hereby made. If applicable, a law firm's check for the petition for extension of time fee is enclosed herewith. If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to charge any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP

Dated: June 18, 2009

/StoychoDDraganoff#56181/
Stoycho D. Draganoff
Reg. No. 56,181

2055 Gateway Place, Suite 550
San Jose, California 95110-1089
Telephone No.: (408) 414-1080 ext. 208
Facsimile No.: (408) 414-1076